On the minimum of a positive polynomial over the standard simplex

Gabriela Jeronimo[a,b,*] Daniel Perrucci[a,*]

[a] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales,
Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

[b] CONICET - Argentina

June 23, 2009

Abstract

We present a new positive lower bound for the minimum value taken by a polynomial P with integer coefficients in k variables over the standard simplex of $\mathbb{R}^k$, assuming that P is positive on the simplex. This bound depends only on the number of variables k, the degree d and the bitsize τ of the coefficients of P and improves all previous bounds for arbitrary polynomials which are positive over the simplex.

1 Introduction

In the last years, the problem of determining the positivity of a polynomial in k variables with real coefficients in (a subset of) $\mathbb{R}^k$ has been studied extensively with different approaches (see, for instance, [12]). One of them consists in exhibiting a *certificate of positivity*, that is to say, an algebraic identity showing explicitly that the polynomial is positive over the considered set (see [3]). In order to construct these certificates of positivity, it is useful to know an *a priori* lower bound for the minimum of a polynomial which only takes positive values on the set (see for instance [11], [14], [9]). For bounded subsets of $\mathbb{R}^k$, such a bound can be obtained by means of Lojasiewicz inequalities (see [3] or [15]), as it is done in [5] for the case of the standard simplex of $\mathbb{R}^k$. However, these bounds involve a universal constant.

This papers considers the problem of finding an explicit lower bound for the minimum of a polynomial $P \in \mathbb{Z}[X_1, \dots, X_k]$ over the standard k-dimensional simplex $\Delta_k = \{x \in \mathbb{R}^k_{\ge 0} \mid \sum_{i=1}^k x_i \le 1\}$, assuming that P takes only positive values on Δ_k, which depends only on the number of variables k of P, its degree d, and an upper bound τ for the bitsize of its coefficients.

Under non-degeneracy conditions, a lower bound of this kind can be obtained by applying Canny's gap theorem ([4]). In [6], an improved gap theorem is proved and,

[*] Partially supported by the following Argentinian research grants: UBACyT X847 (2006-2010) and PIP CONICET 5852/05.

consequently, a better bound under the same assumptions is derived. The best known lower bound for the minimum with no extra assumptions on P was given in [1], where the minimum is estimated by means of an analysis of the values that the polynomial takes on the boundary of the simplex and its critical values in the interior.

Here we present a new lower bound for the minimum in the general case which improves the previous ones. Our main result is the following:

Theorem 1 *For every $P \in \mathbb{Z}[X_1, \dots, X_k]$ with degree d and coefficients of bitsize at most τ which only takes positive values over the standard simplex Δ_k, we have*

$$\min_{\Delta_k} P \geq 2^{-(\tau+1)d^{k+1}} d^{-(k+1)d^k} \binom{d+k}{k+1}^{-d^k(d-1)}$$

Taking into account that $\binom{d+k}{k+1} \leq d^{k+1}$, we obtain the simplified bound

$$\min_{\Delta_k} P \geq 2^{-(\tau+1)d^{k+1}} d^{-(k+1)d^{k+1}}.$$

Our approach combines the application of the critical point method as in [1] with deformation techniques similar to those used in [8] to compute critical values. This deformation-based approach enables us to work, even in degenerate cases, with a polynomial system defining the critical points of an associated polynomial instead of taking the sum of squares of the polynomials involved, as it is done in [1] leading to an artificial degree growth. Moreover, we estimate the values that the polynomial takes at the critical points by computing upper bounds on the coefficients of the characteristic polynomial of a multiplication map in the associated quotient algebra, with no need of a previous explicit description of these critical points.

2 A lower bound for the minimum

For $k \in \mathbb{N}$, consider the k-dimensional standard simplex

$$\Delta_k = \Big\{ x \in \mathbb{R}^k_{\geq 0} \mid \sum_{i=1}^{k} x_i \leq 1 \Big\},$$

and for $k, d, \tau \in \mathbb{N}$, let

$$\mathcal{A}_{k,d,\tau} = \{ P \in \mathbb{Z}[X_1, \dots, X_k] \mid \deg(P) \leq d,\ h(P) \leq \tau,\ P(x) > 0\ \forall\, x \in \Delta_k \}$$

(here, $\deg(P)$ denotes the total degree of P and $h(P)$ the maximum bitsize of its coefficients). We are interested in computing an explicit lower bound for

$$m_{k,d,\tau} = \min\{ \min_{\Delta_k} P \mid P \in \mathcal{A}_{k,d,\tau} \},$$

the minimum value over the standard simplex of a polynomial $P \in \mathcal{A}_{k,d,\tau}$, depending only on k, d and τ.

We will analyze first the case where P attains its minimum only at interior points of the simplex and then, we will proceed recursively to deal with the case where the minimum is attained at a point of the boundary. In order to do this, we consider

$$\begin{aligned}\mathcal{A}_{k,d,\tau}^{(b)} &= \{P \in \mathcal{A}_{k,d,\tau} \mid \exists z \in \partial\Delta_k \text{ such that } P(z) = \min_{\Delta_k} P\},\\ \mathcal{A}_{k,d,\tau}^{(0)} &= \mathcal{A}_{k,d,\tau} \setminus \mathcal{A}_{k,d,\tau}^{(b)}.\end{aligned}$$

2.1 The deformation

Fix a polynomial $P \in \mathcal{A}_{k,d,\tau}^{(0)}$. Let $Q(X) = \sum_{i=1}^{k} \frac{1}{d+1} X_i^{d+1}$ and $F(t,X) = P(X) + tQ(X)$. For $i = 1, \dots, k$, let

$$F_i(t,X) = \frac{\partial F}{\partial X_i} = \frac{\partial P}{\partial X_i} + tX_i^d.$$

Following [8], consider the variety $\widehat{V} = V(F_1, \dots, F_k) \subseteq \mathbb{A}^1_{\mathbb{C}} \times \mathbb{A}^k_{\mathbb{C}}$ and its decomposition

$$\widehat{V} = V^{(0)} \cup V^{(1)} \cup V,$$

where $V^{(0)}$ is the union of the irreducible components of $\widehat{V}$ contained in $\{t = 0\}$, $V^{(1)}$ is the union of the irreducible components of $\widehat{V}$ contained in $\{t = t_0\}$ for some $t_0 \in \mathbb{C} \setminus \{0\}$ and V is the union of the remaining irreducible components of $\widehat{V}$.

Lemma 2 *There exists $z_0 \in \Delta_k$ such that $P(z_0) = \min_{\Delta_k} P$ and $(0, z_0) \in V$.*

Proof. Let $\varepsilon > 0$ such that $\varepsilon < |t_0|$ for every $t_0 \in \pi_t(V^{(1)})$ (here, $\pi_t : \mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^1$ denotes the projection to the first coordinate t). Let $(t_n)_{n\in\mathbb{N}}$ be a decreasing sequence of positive real numbers with $t_1 < \varepsilon$ and $\lim_{n\to\infty} t_n = 0$. For every $n \in \mathbb{N}$, let $w_n \in \Delta_k$ such that $F(t_n, w_n) = \min_{\Delta_k} F(t_n, -)$. We may assume that the sequence $(w_n)_{n\in\mathbb{N}}$ converges to a point $z_0 \in \Delta_k$. Therefore, for every $z \in \Delta_k$, we have

$$P(z_0) = F(0, z_0) = \lim_{n\to\infty} F(t_n, w_n) \le \lim_{n\to\infty} F(t_n, z) = F(0, z) = P(z).$$

We conclude that $P(z_0) = \min_{\Delta_k} P$. As $P \in \mathcal{A}_{k,d,\tau}^{(0)}$, the point z_0 lies in the interior Δ_k° of Δ_k and, therefore, $w_n \in \Delta_k^\circ$ for $n \gg 0$. Then, for every $n \gg 0$, w_n is a local minimum of $F(t_n, -)$ and so, $F_i(t_n, w_n) = 0$ for $i = 1, \dots, k$. By the choice of t_1, it follows that $(t_n, w_n) \in V$ for $n \gg 0$ and therefore, $(0, z_0) \in V$. □

Assume $P = \sum_{|\alpha|\le d} a_\alpha X^\alpha$ and let $R \in \mathbb{Z}[X]$ be the polynomial

$$R(X) = d \cdot P(X) - \sum_{1\le i\le k} X_i \frac{\partial P}{\partial X_i}(X) = \sum_{|\alpha|\le d-1} (d - |\alpha|) a_\alpha X^\alpha.$$

Note that for a point z_0 as in Lemma 2, since $\frac{\partial P}{\partial X_i}(z_0) = 0$ for $1 \le i \le k$, we have that $R(z_0) = d \cdot P(z_0)$.

Let $W = \mathbb{C}(t)[X_1, \dots, X_k]/(F_1, \dots, F_k)$, which is a $\mathbb{C}(t)$-vector space of dimension d^k. Moreover, if

$$U = \{\gamma = (\gamma_1, \dots, \gamma_k) \in \mathbb{Z}^k \mid 0 \le \gamma_i \le d - 1 \text{ for every } 1 \le i \le k\},$$

we have that $\{X^\gamma \mid \gamma \in U\}$ is a basis of W. For a polynomial $g \in \mathbb{Z}[X]$, m_g will denote the multiplication map $m_g : W \to W$, $m_g([f]) = [g \cdot f]$, and $\chi(m_g) \in \mathbb{C}(t)[Y]$ the characteristic polynomial of this linear map.

We are going to show that $\chi(m_R)(t, Y) = S(t, Y)/t^l$, where $S(t, Y) \in \mathbb{Q}[t, Y]$, $l \in \mathbb{N}_0$, and $S(0, Y) \not\equiv 0$. Then, since $\chi(m_R)(t, R(X)) \in (F_1, \dots, F_k)\mathbb{C}(t)[X_1, \dots, X_k]$, we have that there is a polynomial $\alpha(t) \in \mathbb{C}[t]$ such that $\alpha(t)S(t, R(X)) \in (F_1, \dots, F_k)\mathbb{C}[t, X_1, \dots, X_k]$. Therefore, $S(t, R(X)) \in I(V)$ and so, $S(0, R(z_0)) = 0$. The bound on the minimum of the polynomial P over the standard simplex will be obtained from upper bounds on the size of the coefficients of $S(0, Y)$.

2.2 Estimates for computations in the quotient algebra

In order to analyze the characteristic polynomial $\chi(m_R)$, we start by studying re-writing techniques in the basis $\{X^\gamma \mid \gamma \in U\}$ of W. We follow the approach in [2, Chapter 12].

For every $\beta \in \mathbb{N}_0^k$, the residue class of the monomial X^β in W can be written in the form $X^\beta = \sum_{\gamma \in U} x_{\beta,\gamma} X^\gamma$ for some elements $x_{\beta,\gamma} \in \mathbb{C}(t)$. Moreover, we have:

Lemma 3 *For every $\beta \in \mathbb{N}_0^k$ and every $\gamma \in U$, there is a univariate polynomial $c_{\beta,\gamma} \in \mathbb{Z}[T]$ such that $x_{\beta,\gamma} = c_{\beta,\gamma}(\frac{1}{t})$. Moreover, if $\beta \notin U$, $c_{\beta,\gamma} = 0$ for every γ with $|\gamma| \geq |\beta|$.*

Proof. First note that, for $\beta \in U$, the identity holds trivially with $c_{\beta,\gamma} = 0$ if $\gamma \neq \beta$ and $c_{\beta,\gamma} = 1$ if $\gamma = \beta$.

For $\beta \notin U$, there exists an index i such that $\beta_i \geq d$ and, so, $\beta = \tilde{\beta} + de_i$ with $\tilde{\beta} \in \mathbb{N}_0^k$. We proceed by induction on $|\beta|$, starting with $|\beta| = d$. In this case, we have that $\beta = de_i$ and the following identity holds in W:

$$X_i^d = \sum_{|\alpha|<d} -a_{\alpha+e_i}(\alpha_i + 1)\frac{1}{t} X^\alpha. \tag{1}$$

We conclude that $c_{\beta,\gamma} = -a_{\gamma+e_i}(\gamma_i + 1)T$ if $|\gamma| < d = |\beta|$ and $c_{\beta,\gamma} = 0$ if $|\gamma| \geq d = |\beta|$.

Now, if $\beta = \tilde{\beta} + de_i$, we have

$$X^\beta = X_i^d X^{\tilde{\beta}} = \sum_{|\alpha|<d} -a_{\alpha+e_i}(\alpha_i + 1)\frac{1}{t} X^{\alpha+\tilde{\beta}};$$

therefore,

$$\begin{aligned} X^\beta &= \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\in U} -a_{\alpha+e_i}(\alpha_i+1)\frac{1}{t} X^{\alpha+\tilde{\beta}} + \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} -a_{\alpha+e_i}(\alpha_i+1)\frac{1}{t} \sum_{\gamma\in U} x_{\alpha+\tilde{\beta},\gamma} X^\gamma \\ &= \sum_{\gamma\in U,\, \gamma=\alpha+\tilde{\beta},\, |\alpha|<d} -a_{\alpha+e_i}(\alpha_i+1)\frac{1}{t} X^\gamma + \sum_{\gamma\in U} \Big(\sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} -a_{\alpha+e_i}(\alpha_i+1)\frac{1}{t}\, x_{\alpha+\tilde{\beta},\gamma} \Big) X^\gamma. \end{aligned} \tag{2}$$

Note that for every α such that $|\alpha| < d$, we have that $|\alpha + \tilde{\beta}| = |\alpha| + |\tilde{\beta}| < d + |\beta| - d = |\beta|$; then, by our inductive assumption, it follows that $x_{\alpha+\tilde{\beta},\gamma} = 0$ whenever $\alpha + \tilde{\beta} \notin U$ and $|\alpha + \tilde{\beta}| \leq |\gamma|$. Using the previous identity, this implies that $x_{\beta,\gamma} = 0$ for every $\gamma \in U$ with $|\gamma| \geq |\beta|$.

The inductive assumption also states that $x_{\alpha+\tilde{\beta},\gamma} = c_{\alpha+\tilde{\beta},\gamma}(\frac{1}{t})$ for every α with $|\alpha| < d$ and every $\gamma \in U$; therefore, taking into account identity (2), for every $\gamma \in U$ with $|\gamma| < |\beta|$, we have that $x_{\beta,\gamma} = c_{\beta,\gamma}(\frac{1}{t})$, where

$$c_{\beta,\gamma} = \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} -a_{\alpha+e_i}(\alpha_i + 1)c_{\alpha+\tilde{\beta},\gamma}T \in \mathbb{Z}[T] \tag{3}$$

if $\gamma \neq \alpha + \tilde{\beta}$ for every α with $|\alpha| < d$, and

$$c_{\beta,\gamma} = -a_{(\tilde{\alpha}+e_i)}(\tilde{\alpha}_i + 1)T + \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} -a_{\alpha+e_i}(\alpha_i + 1)c_{\alpha+\tilde{\beta},\gamma}T \in \mathbb{Z}[T] \tag{4}$$

if $\gamma = \tilde{\alpha} + \tilde{\beta}$ with $|\tilde{\alpha}| < d$. □

Notation 4 *For a univariate polynomial $c \in \mathbb{Z}[T]$, we use the notation c_l to indicate the coefficient of the monomial T^l in c.*

Lemma 5 *For every $\beta \in \mathbb{N}_0^k - U$ and every $\gamma \in U$ with $|\gamma| < |\beta|$, $\deg c_{\beta,\gamma} \leq |\beta| - |\gamma|$ and, for $0 \leq l \leq |\beta| - |\gamma|$,*

$$|c_{\beta,\gamma,l}| \leq 2^{l\tau} d \binom{d+k}{k+1}^{l-1}.$$

Proof. The proof is done by induction on $|\beta|$. If $|\beta| = d$, then $\beta = de_i$ for some index i with $1 \leq i \leq k$ and so, we have that either $c_{\beta,\gamma} = 0$ or $c_{\beta,\gamma} = -a_{\gamma+e_i}(\gamma_i + 1)T$ (see identity (1)). In any case, the result holds.

Suppose now that $|\beta| > d$. There exists an index i such that $\beta = \tilde{\beta} + de_i$ with $\tilde{\beta} \in \mathbb{N}_0^k$. By the inductive hypothesis, for every $|\alpha| < d$ with $\alpha + \tilde{\beta} \notin U$,

$$\deg c_{\alpha+\tilde{\beta},\gamma}T \leq |\alpha + \tilde{\beta}| - |\gamma| + 1 \leq |\beta| - |\gamma|;$$

so, identities (3) and (4) imply that the stated degree bound for $c_{\beta,\gamma}$ holds.

Note that $c_{\beta,\gamma,0} = 0$, and $c_{\beta,\gamma,1} = -(\tilde{\alpha}_i + 1)a_{\tilde{\alpha}+e_i}$ if there exists $\tilde{\alpha} \in \mathbb{N}_0^k$ with $|\tilde{\alpha}| < d$ and $\gamma = \tilde{\alpha} + \tilde{\beta}$, and $c_{\beta,\gamma,1} = 0$ otherwise. In any case, the bound on the coefficient size holds for $l = 0, 1$. Consider now the case $l \geq 2$; from identities (3) and (4), using the inductive assumption we have

$$\begin{aligned}
|c_{\beta,\gamma,l}| &= \Big| \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} -a_{\alpha+e_i}(\alpha_i + 1)\, c_{\alpha+\tilde{\beta},\gamma,l-1} \Big| \\
&\leq \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U} 2^{\tau}(\alpha_i + 1)2^{(l-1)\tau} d \binom{d+k}{k+1}^{l-2} \\
&= 2^{l\tau} d \binom{d+k}{k+1}^{l-2} \sum_{0\leq e\leq d-1} \sum_{|\alpha|<d,\, \alpha+\tilde{\beta}\notin U,\, \alpha_i=e} (e+1) \\
&\leq 2^{l\tau} d \binom{d+k}{k+1}^{l-2} \sum_{0\leq e\leq d-1} (e+1) \binom{d-1-e+k-1}{k-1}.
\end{aligned}$$

The result follows noticing that

$$\sum_{0\le e\le d-1}(e+1)\binom{d-1-e+k-1}{k-1} = \sum_{0\le e\le d-1}\sum_{0\le j\le e}\binom{d-1-e+k-1}{k-1} =$$

$$= \sum_{0\le j\le d-1}\sum_{j\le e\le d-1}\binom{d-1-e+k-1}{k-1} = \sum_{0\le j\le d-1}\binom{d-1+k-j}{k} = \binom{d+k}{k+1}.$$

□

2.3 Bounds for traces and characteristic polynomial coefficients

To estimate the size of the coefficients of the characteristic polynomial $\chi(m_R) \in \mathbb{Z}[\frac{1}{t}][Y]$, we will use the following relationship with the traces of the multiplication maps by the powers of R (see for instance [2, Chapter 12]): if $\chi(m_R)(Y) = \sum_{h=0}^{d^k} b_{d^k-h}Y^{d^k-h}$, we have

- $b_{d^k} = 1$,
- for $1 \le h \le d^k$,

$$b_{d^k-h} = -\frac{1}{h}\sum_{n=1}^{h} \operatorname{tr}(m_{R^n})b_{d^k-h+n}. \tag{5}$$

(See also [7] or [13], where this technique has been used for this task and, more generally, for the computation of a rational univariate representation of the solutions to a zero-dimensional polynomial system.)

For $n \in \mathbb{N}$, let $R^n(X) := \sum_{|\alpha|\le(d-1)n} R_\alpha^{(n)}X^\alpha$. Let us observe that

$$\begin{aligned}\sum_{|\alpha|\le d-1}|R_\alpha^{(1)}| &\le \sum_{|\alpha|\le d-1}(d-|\alpha|)|a_\alpha| \le 2^\tau \sum_{0\le e\le d-1}(d-e)\binom{e+k-1}{k-1}\\ &= 2^\tau\sum_{0\le e'\le d-1}(e'+1)\binom{d-1-e'+k-1}{k-1} = 2^\tau\binom{d+k}{k+1},\end{aligned}$$

where the last identity was shown in the proof of Lemma 5; in the general case,

$$\sum_{|\alpha|\le(d-1)n}|R_\alpha^{(n)}| \le \Big(\sum_{|\alpha|\le d-1}|R_\alpha^{(1)}|\Big)^n \le \Big(2^\tau\binom{d+k}{k+1}\Big)^n. \tag{6}$$

In the sequel, for every $n \in \mathbb{N}$, we will use the same notation m_{R^n} to denote the multiplication map by R^n in W or the matrix of this linear map in the basis $\{X^\gamma \mid \gamma \in U\}$. Rows and columns of these matrices will be indexed by the exponent vectors $\gamma \in U$.

From Lemma 3 and the fact that $R \in \mathbb{Z}[X]$, it follows that the entries of the matrices m_{R^n} are polynomials in $\mathbb{Z}[\frac{1}{t}]$ and, therefore, the same holds for their traces.

Lemma 6 *For every $n \in \mathbb{N}$, $\deg_{\frac{1}{t}} \operatorname{tr}(m_{R^n}) \le n(d-1)$ and, for $0 \le l \le n(d-1)$,*

$$|\operatorname{tr}(m_{R^n})_l| \le 2^{(l+n)\tau}d^{k+1}\binom{d+k}{k+1}^{l+n-1}.$$

Proof. For every $n \in \mathbb{N}$ and $\gamma \in U$, $(m_{R^n})_{\gamma,\gamma} = \sum_{|\alpha|\le n(d-1)} R^{(n)}_\alpha c_{\gamma+\alpha,\gamma}\big(\frac{1}{t}\big)$, where $c_{\gamma+\alpha,\gamma}$ is a constant if $\gamma+\alpha \in U$ and $\deg c_{\gamma+\alpha,\gamma} \le |\gamma+\alpha| - |\gamma| = |\alpha| \le n(d-1)$ if $\gamma+\alpha \notin U$. Now,

$$|(m_{R^n})_{\gamma,\gamma,0}| \le \sum_{|\alpha|\le n(d-1)} |R^{(n)}_\alpha c_{\gamma+\alpha,\gamma,0}| = |R^{(n)}_0| = |R^{(1)}_0|^n \le 2^{n\tau} d^n \le 2^{n\tau} d \binom{d+k}{k+1}^{n-1},$$

and, for $1 \le l \le n(d-1)$,

$$\begin{aligned} |(m_{R^n})_{\gamma,\gamma,l}| &\le \sum_{|\alpha|\le n(d-1)} |R^{(n)}_\alpha c_{\gamma+\alpha,\gamma,l}| = \sum_{|\alpha|\le n(d-1),\, \gamma+\alpha\notin U} |R^{(n)}_\alpha c_{\gamma+\alpha,\gamma,l}| \\ &\le \sum_{|\alpha|\le n(d-1)} |R^{(n)}_\alpha|\, 2^{l\tau} d \binom{d+k}{k+1}^{l-1} \le 2^{(l+n)\tau} d \binom{d+k}{k+1}^{l+n-1}, \end{aligned}$$

where the last inequality follows from (6). The stated inequalities are now a consequence of the fact that the dimension of W is d^k. □

We are now ready to find upper bounds for the size of the coefficients of the characteristic polynomial $\chi(m_R) \in \mathbb{Z}[\frac{1}{t}][Y]$.

Lemma 7 *For $0 \le h \le d^k$, $\deg_{\frac{1}{t}} b_{d^k-h} \le h(d-1)$ and, for $0 \le l \le h(d-1)$,*

$$|b_{d^k-h,l}| \le 2^{(l+h)(\tau+1)} d^{(k+1)h} \binom{d+k}{k+1}^{l}.$$

The last inequalities are strict for $h \ge 1$.

Proof. Let us prove first the degree bound. The proof is done by induction on h and using the recursive formula (5) for the coefficients b_{d^k-h}. For $h=0$, the result holds. Now, for $h>0$, for every $1 \le n \le h$, by Lemma 6 and the inductive assumption, $\deg(\mathrm{tr}(m_{R^n}) b_{d^k-h+n}) \le n(d-1) + (h-n)(d-1) = h(d-1)$; therefore, $\deg b_{d^k-h} \le h(d-1)$.

Now we prove the bound on the size of the coefficients. For $h=0$, the result is clear. For $h \ge 1$,

$$\begin{aligned} |b_{d^k-h,l}| &= \frac{1}{h}\Big|\sum_{n=1}^{h} \sum_{\substack{l_1+l_2=l\\ 0\le l_1\le n(d-1)\\ 0\le l_2\le (h-n)(d-1)}} \mathrm{tr}(m_{R^n})_{l_1} b_{d^k-h+n,l_2}\Big| \\ &\le \frac{1}{h}\sum_{n=1}^{h} \sum_{\substack{l_1+l_2=l\\ 0\le l_1\le n(d-1)\\ 0\le l_2\le (h-n)(d-1)}} 2^{(l_1+n)\tau} d^{k+1}\binom{d+k}{k+1}^{l_1+n-1} 2^{(l_2+h-n)(\tau+1)} d^{(k+1)(h-n)}\binom{d+k}{k+1}^{l_2} \\ &= 2^{(l+h)\tau} d^{k+1}\binom{d+k}{k+1}^{l-1} \frac{1}{h}\sum_{n=1}^{h}\binom{d+k}{k+1}^{n} 2^{h-n} d^{(k+1)(h-n)} \sum_{\substack{l_1+l_2=l\\ 0\le l_1\le n(d-1)\\ 0\le l_2\le (h-n)(d-1)}} 2^{l_2} \\ &< 2^{(l+h)\tau} d^{k+1}\binom{d+k}{k+1}^{l-1}\binom{d+k}{k+1} 2^{h-1} d^{(k+1)(h-1)}\, 2^{l+1} \\ &= 2^{(l+h)(\tau+1)} d^{(k+1)h}\binom{d+k}{k+1}^{l}. \end{aligned}$$

□

2.4 Obtaining the bound

As explained in Subsection 2.1, from the characteristic polynomial $\chi(m_R)$, we can obtain a univariate polynomial having $R(z_0)$ as one of its roots; thus, we get a lower bound for this value in terms of the size of the coefficients of this polynomial.

Proposition 8 *Let z_0 be as in Lemma 2. Then,*

$$\frac{1}{P(z_0)} \le 2^{d^{k+1}(\tau+1)} d^{(k+1)d^k} \binom{d+k}{k+1}^{d^k(d-1)}.$$

Proof. Take $l_0 := \max_{0\le h\le d^k} \deg b_{d^k-h}$. Then, $\chi(m_R) = \frac{S(t,Y)}{t^{l_0}}$, where

$$S(t,Y) = t^{l_0}\sum_{h=0}^{d^k} b_{d^k-h}(\frac{1}{t})Y^{d^k-h} = \sum_{h=0}^{d^k}\sum_{l=0}^{l_0} b_{d^k-h,l}\, t^{l_0-l}\, Y^{d^k-h} \in \mathbb{Z}[t,Y],$$

and, therefore, $S(0,Y) = \sum_{h=0}^{d^k} b_{d^k-h,l_0} Y^{d^k-h} \in \mathbb{Z}[Y]$. Since $(0,z_0) \in V$, we have that $S(0,R(z_0)) = 0$, which implies that $\frac{1}{R(z_0)}$ is a root of the polynomial $\sum_{h=0}^{d^k} b_{d^k-h,l_0} Y^h$.

If $l_0 > (d^k-1)(d-1)$, then $b_{d^k-h,l_0} = 0$ for every $0 \le h \le d^k-1$, and so $b_{0,l_0}\big(\frac{1}{R(z_0)}\big)^{d^k} = 0$, which is impossible since both factors are nonzero. Let $h_1 := \max\{h \mid b_{d^k-h,l_0} \ne 0\} \le d^k$. By [10, Prop. 2.5.9],

$$\frac{1}{R(z_0)} \le \max_{0\le h\le h_1-1} \left|\frac{b_{d^k-h,l_0}}{b_{d^k-h_1,l_0}}\right| + 1.$$

Since $b_{d^k-h_1,l_0} \in \mathbb{Z}-\{0\}$ and the size inequalities in Lemma 7 are strict for $h>0$,

$$\frac{1}{d\cdot P(z_0)} = \frac{1}{R(z_0)} \le 2^{(d^k-1)d(\tau+1)} d^{(k+1)(d^k-1)} \binom{d+k}{k+1}^{(d^k-1)(d-1)},$$

which implies the result. □

By Lemma 2 and Proposition 8, we deduce the following lower bound for the minimum of a positive polynomial over the standard simplex in the case this minimum is attained only at interior points of the simplex:

Proposition 9 *Let $P \in \mathcal{A}^{(0)}_{k,d,\tau}$. Then*

$$\min_{\Delta_k} P \ge 2^{-(\tau+1)d^{k+1}} d^{-(k+1)d^k} \binom{d+k}{k+1}^{-d^k(d-1)}.$$

2.5 Proof of the main result

The case where the minimum is attained at a point of the boundary of Δ_k can be dealt with recursively, since the facets of Δ_k are standard $(k-1)$-dimensional simplices.

We are now ready to prove the main result of the paper.

Proof of Theorem 1. We argue by induction on k. For $k=1$, the bound is a consequence of Proposition 9 and the fact that $P(0)\geq 1$ and $P(1)\geq 1$ for every $P\in\mathcal{A}_{k,d,\tau}$.

Assume now $k>1$ and let $P\in\mathcal{A}_{k,d,\tau}$. When $d=1$, P is a linear affine polynomial and so, the minimum is attained at a vertex of the simplex, which implies that it is an integer. Then, $m_{k,1,\tau}\geq 1$ for every k,τ. Thus, we may assume $d\geq 2$.

If $P\in\mathcal{A}^{(0)}_{k,d,\tau}$, the bound follows from Proposition 9. Suppose $P\in\mathcal{A}^{(b)}_{k,d,\tau}$ and let $z\in\partial\Delta_k$ with $P(z)=\min_{\Delta_k}P$. If $z_i=0$ for some $1\leq i\leq k$, the polynomial P_i obtained by evaluating $X_i=0$ in P satisfies $P_i\in\mathcal{A}_{k-1,d,\tau}$ and

$$P(z)=P_i(z_1,\dots,\widehat{z_i},\dots,z_n)\geq m_{k-1,d,\tau}\geq 2^{-(\tau+1)d^k}d^{-kd^{k-1}}\binom{d+k-1}{k}^{-d^{k-1}(d-1)}$$

(here, $(z_1,\dots,\widehat{z_i},\dots,z_n)\in\Delta_{k-1}$ is the point obtained by removing the ith coordinate from $z\in\Delta_k$). On the other hand, if $\sum_{i=1}^k z_i=1$, consider the polynomial $\widetilde{P}=P(X_1,\dots,X_{k-1},1-(X_1+\cdots+X_{k-1}))$. By [1, Lemma 2.3], $\widetilde{P}\in\mathcal{A}_{k-1,d,\tau+1+d\log k}$ and, therefore

$$P(z)=\widetilde{P}(z_1,\dots,z_{k-1})\geq m_{k-1,d,\tau+1+d\log k}\geq 2^{-(\tau+2+d\log k)d^k}d^{-kd^{k-1}}\binom{d+k-1}{k}^{-d^{k-1}(d-1)}.$$

In order to finish the proof, it suffices to show that for every $d\geq 2$, and every $k\in\mathbb{N}$,

$$2^{d^k(\tau+2+d\log k)}d^{kd^{k-1}}\binom{d+k-1}{k}^{d^{k-1}(d-1)}\leq 2^{d^{k+1}(\tau+1)}d^{(k+1)d^k}\binom{d+k}{k+1}^{d^k(d-1)}. \tag{7}$$

First, we show by induction on d, that for every $d\geq 2$ and every $k\in\mathbb{N}$, the inequality $k^{2d-1}\leq 2^{d^2-2d}d^{(k+1)d-k}$ holds: the case $d=2$ follows easily; in addition,

$$\begin{aligned}k^{2(d+1)-1} &\leq 2^{k+4}k^{2d-1}\leq 2^{2d-1}d^{k+1}k^{2d-1}\leq 2^{2d-1}d^{k+1}2^{d^2-2d}d^{(k+1)d-k}\\ &= 2^{(d+1)^2-2(d+1)}d^{(k+1)(d+1)-k}\leq 2^{(d+1)^2-2(d+1)}(d+1)^{(k+1)(d+1)-k}.\end{aligned}$$

Then, $k^{2d^k-d^{k-1}}=(k^{2d-1})^{d^{k-1}}\leq(2^{d^2-2d}d^{(k+1)d-k})^{d^{k-1}}=2^{d^{k+1}-2d^k}d^{(k+1)d^k-kd^{k-1}}$ and, therefore,

$$2^{2d^k}k^{d^{k+1}}d^{kd^{k-1}}\binom{d+k-1}{k}^{d^{k-1}(d-1)}\leq 2^{d^{k+1}}d^{(k+1)d^k}k^{d^{k+1}-2d^k+d^{k-1}}\binom{d+k-1}{k}^{d^{k-1}(d-1)}.$$

Since $\binom{d+k}{k+1}\geq k$ and $\binom{d+k}{k+1}\geq\binom{d+k-1}{k}$, we conclude that

$$2^{2d^k}k^{d^{k+1}}d^{kd^{k-1}}\binom{d+k-1}{k}^{d^{k-1}(d-1)}\leq 2^{d^{k+1}}d^{(k+1)d^k}\binom{d+k}{k+1}^{d^k(d-1)},$$

which implies that inequality (7) holds. □

3 An example

The following example shows that the doubly exponential character of the bound is unavoidable.

Example 10 *Let τ and d be even positive integers, $d \geq 4$. Consider the polynomial*

$$P(X_1, \ldots, X_k) = (2^{\tau/2} X_1 - 1)^2 + (X_2 - X_1^{d/2})^2 + \cdots + (X_k - X_{k-1}^{d/2})^2 + X_k^d.$$

Note that P is positive over $\mathbb{R}^k$. Substituting $X_i = 2^{-\frac{\tau}{2}(\frac{d}{2})^{i-1}}$ for $i = 1, \ldots, k$, it follows that the minimum of P over the standard simplex of $\mathbb{R}^k$ is lower than or equal to $2^{-\tau(\frac{d}{2})^k}$.

Acknowledgements. The authors wish to thank Marie-Françoise Roy for suggesting them the problem and a possible approach to it. They also acknowledge Saugata Basu, Richard Leroy and Marie-Françoise Roy for their comments on a first version of the paper.

References

[1] S. Basu, R. Leroy, and M.-F. Roy. A bound on the minimum of a real positive polynomial over the standard simplex.

[2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics.* 2nd. ed. Springer-Verlag, Berlin, 2006.

[3] J. Bochnak, M. Coste, M. F. Roy, *Géométrie algébrique réelle.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 12. Springer-Verlag, Berlin, 1987.

[4] J. Canny, The complexity of robot motion planning, MIT press, 1987.

[5] J.A. de Loera, F. Santos, An effective version of Pölya's theorem on positive definite forms, J. Pure and Appl. Algebra 108 (3) (1996), 231-240.

[6] I.Z. Emiris, B. Mourrain, E. Tsigaridas. The DMM bound: multivariate (aggregate) separation bounds. Manuscript.

[7] L. González-Vega, G. Trujillo, Using symmetric functions to describe the solution set of a zero dimensional ideal. Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), 232-247, Lecture Notes in Comput. Sci., 948, Springer, Berlin, 1995.

[8] G. Jeronimo, D. Perrucci, J. Sabia. On sign conditions over real multivariate polynomials. To appear in Discrete Comput. Geom. DOI: 10.1007/s00454-009-9200-4.

[9] R. Leroy, Certificats de positivité et minimisation polynomiale dans la base de Bernstein multivariée, PhD. Thesis, Université de Rennes 1, 2008.

[10] M. Mignotte, D. Stefanescu, *Polynomials. An algorithmic approach.* Springer Series in Discrete Mathematics and Theoretical Computer Science. Springer-Verlag Singapore, Singapore; Centre for Discrete Mathematics & Theoretical Computer Science, Auckland, 1999.

[11] V. Powers, B. Reznick, A new bound for Plya's theorem with applications to polynomials positive on polyhedra. Effective methods in algebraic geometry (Bath, 2000). J. Pure Appl. Algebra 164 (2001), no. 1-2, 221–229.

[12] A. Prestel, C.N. Delzell, *Positive polynomials. From Hilbert's 17th problem to real algebra.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2001.

[13] F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, Appl. Algebra Eng. Commun. Comput. 9, No.5, 433-461 (1999).

[14] M. Schweighofer, On the complexity of Schmdgen's positivstellensatz. J. Complexity 20 (2004), no. 4, 529–543.

[15] P. Solernó, Effective Łojasiewicz inequalities in semialgebraic geometry. Appl. Algebra Engrg. Comm. Comput. 2 (1991), No. 1, 2-14.